UK Parliament
POST

**POSTnote 731**

By Vincent Saverat,
Simon Brawley
23 September 2024

# Biometric data: Misuse, use, and collation


## Overview

- Biometric data is a type of personal information that allows the unique identification of a person. The most common forms of biometric data rely on fingerprints, face geometry, and voice.
- Biometric data is commonly used to unlock personal devices, speed up passport checks, or verify someone's identity for online banking.
- According to a 2023 survey, 33% of respondents in the UK preferred biometric verification as a sign-in method over using a password or an authentication application.
- Biometric data is considered "special category personal data" under the Data Protection Act 2018 and receives extra legal protection. However, researchers and think tanks have indicated that additional legal safeguards may be required, for instance, for the use of modern biometric systems such as facial recognition.
- Developments in artificial intelligence have made new uses of biometric data possible. It has been suggested that personal information such as age, ethnicity, sexuality, or emotions, can be inferred from biometric data. This could have a range of ethical implications, including negative implications for privacy and other civil liberties.

# Background

Biometric data is a type of personal information that allows the unique identification of a person. It is defined in UK law as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person".[a] [1,2]

Physical and physiological biometric data includes information on fingerprints or faceprints, while behavioural biometric data includes information on voiceprints or gait analysis (see Box 1).[b] [8,9]

According to a 2023 study,[c] respondents increasingly prefer biometric verification for device sign-in (33%) over using a password (15%) or an authenticator application[d] (5%).[11] The most common methods for biometric verification on personal devices such as smartphones and laptops are face and fingerprint verification.[12] To create a biometric record and to verify the user, a series of processes take place (see Table 1).

Industry estimates suggest that the global "passwordless verification"[e] market was worth over £12.5 billion in 2023 and is expected to reach a value of £46 billion by 2032.[14] This is mostly due to increased adoption.[14]

Unlike passwords, biometric data is linked to the physical or behavioural characteristics of a person. If stolen, it is impossible for a user to get new biometric characteristics. Due to its sensitive nature, biometric data is considered "special category personal data"[f] [15] and receives extra protection under the Data Protection Act (DPA) 2018[1] and the UK General Data Protection Regulation (UK GDPR) (see section on "UK regulatory environment for biometric data").[2,16]

Developments in artificial intelligence (AI) have made possible new uses of biometric data, including live facial recognition and emotion analysis. Academics and think tanks have expressed concerns that these new tools could require enhanced individual protections and further regulations.[17–22]

---

[a] Biometric data is defined in the UK under the Data Protection Act 2018, and in the EU under General Data Protection Regulation.

[b] Genetic data is not considered biometric data under the Data Protection Act 2018. However, genetic data is considered biometric data by international standards,[3,4] previous UK laws (Protection of Freedoms Act 2012),[5] and Scottish law (Scottish Biometrics Commissioner Act 2020).[6,7]

[c] A survey by the FIDO Alliance of 10,000 consumers in U.S., U.K., France, Germany, Australia, Singapore, Japan, South Korea, India and China

[d] An authenticator application is a software which generates secure codes one can use to sign-in to their online accounts.[10]

[e] Passwordless verification (also known as passwordless authentication) is a verification method allowing a user to access a system with a evidence other than a password such as personal identifying numbers (PINs), security tokens, or biometric data (for instance, fingerprint verification).[13,14]

[f] Biometric data is considered special category data where the purpose test of unique identification is met.

### Box 1: Types of biometric data and sign-in methods

The most common biometric data for personal device sign-in are:

- **Fingerprints**: No two fingerprints have ever been found to be identical, including between identical twins.[23] Fingerprint uniqueness has been used since 1892 to solve criminal cases[23] and can be used to unlock personal devices such as smartphones and laptops. Examples include Apple Touch ID and Windows Hello.[24–26]
- **Voiceprints**: Everyone has a unique voice due to differences in vocal tract shape, larynx size, speaking rhythm and intonation style.[27] Voice frequencies can be converted into a unique mathematical formula called a voiceprint.[28] Voiceprint verification is used to access banking and public services (for instance, HMRC).[29–34]

**Faceprints**: Facial landmarks, such as the distance between the eyes, the distance from forehead to chin, or the shape of cheekbones can be converted into a unique mathematical formula called a faceprint.[35] Faceprint verification can be used for border control checks[36] or for unlocking personal devices. Examples include Apple Face ID and Windows Hello.[35]

# What is biometric data used for?

While biometric verification asks "Is this person who they claim to be?", biometric identification asks "Who is this person?".[37]

## Biometric verification

Biometric verification is the comparison of biometric features of a person with previously stored biometric data. It is used to confirm that they are who they claim to be (see Table 1).[3] It is also known as 'one-to-one comparison'. This process is used in a variety of ways.

| Table 1: Biometric enrolment and verification | |
|---|---|
| **1. Biometric sample** | A digital capture of someone's biological or behavioural characteristics is made using a device such as a camera, a fingerprint scanner, or a microphone.[3] |
| **2. Biometric feature extraction** | Characteristics[g] of the biometric sample are examined.[3] For instance, during the Apple Face ID verification, the built-in face camera examines 30,000 dots from the user's face.[38] The mathematical representation of the location of these dots is a set of biometric features.[h] |
| **3. Biometric template** | A set of biometric features are stored for reference. Users' biographical information[i] can also be stored. It will be used later to prove someone's identity.[3] |
| **4. Encryption** | The biometric template is encrypted to make it difficult to reconstruct a fingerprint or a faceprint from the mathematical representation.[24,35,40] |
| **5. Storage** | **Personal devices**: biometric data is stored on the device and the original biometric capture (for instance, someone's face or fingerprint) is deleted.[41]<br><br>**Servers**: the biometric template is stored in a server and can be accessed remotely to check someone's identity on different sites (for instance, international border checks). It is also easier to update the software that compares the stored biometric template to the biometric data from a user.[41] |
| **6. Verification** | To verify a user's identity, the biometric model captured at the login step is compared to the biometric template of the user. The system then uses a comparison algorithm to decide whether these two biometric models are sufficiently similar to be from the same person.[42] |
| **7. De-enrolment** | Irreversible destruction of the stored biometric template from a personal device or a database.[3] This can be done when a person withdraws their consent or if they make an erasure request.[j] [43,44] |

[g] To meet international security standards, these characteristics need to be repeatable (almost identical between several captures from the same individual) and distinctive (very different from someone else's captures).[3]

[h] Biometric features take the form of a list of numbers readable by biometric algorithms, not by people.[39]

[i] Biographical information can be a person's name, nationality, date of birth, or place of birth.

[j] Exemptions from the right to erasure are detailed in the Data Protection Act 2018.[43] For instance, the right to erasure does not apply if biometric data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.[43]

## British e-Passport

The first British e-Passport was issued in 2006 (also known as a biometric passport). It comprises an electronic chip in which the biographical information[k] and faceprint of the passport holder are embedded.[45] By 2016, all British passports were e-Passports, with over 45 million British e-Passport holders in 2022.[l] [46]

E-Passports can be used with an automated border control system known as eGates.[36] As of March 2024, there were over 270 eGates in place at 15 air and rail ports to facilitate travel into the UK.[36] eGates are automated barriers which compare the faceprint stored in the e-Passport with a photo taken at the time of entry.[47,48]

## Banking

Along with commonly used biometric verification methods such as fingerprints and facial recognition, voice verification offers an additional route for securely accessing banking services over the phone.[49]

Barclays was the first UK bank to use voice verification for some of its customers in 2013.[49] HSBC and Lloyds Banking Group[m] introduced voice verification in 2016[30] and 2018,[32] respectively.

HSBC serves 14.5 million customers in the UK, of which 2 million are active users of its voice verification system.[50] HSBC claims its voice verification system prevented £395 million worth of telephone fraud between 2016 and 2019.[50]

In 2017, a BBC article highlighted potential issues with the HSBC voice verification system when a journalist claimed that his non-identical twin brother managed to access his account by mimicking his brother's voice.[51]

In response, a HSBC spokesperson noted that twins do have similar voiceprints but that this technology is more secure than PINs and passwords and has led to a significant reduction in fraud.[51]

## HM Revenue & Customs

In 2017, HM Revenue and Customs (HMRC) introduced a voice verification system to speed up customer verification when calling the tax credits[n] or Self Assessment[o] helplines.[34] By 2018, almost 7 million users were enrolled in the HMRC voice verification system.[52]

In 2018, Big Brother Watch, a UK civil liberties campaign group, reported that HMRC failed to receive explicit consent to store 5 million user voice records.[53] In May 2019, the Information Commissioner's Office (ICO) considered the HMRC voice verification system to be non-compliant with UK GDPR and requested HMRC to delete the

[k] Biographical information can include a person's name, nationality, date of birth, or place of birth.

[l] Only e-Passports were issued in the UK after 2006.[45]

[m] Lloyds Banking Group includes Lloyds Bank, Halifax, and Bank of Scotland.

[n] This includes claims for child tax credits and work tax credits.

[o] Self Assessment is HMRC's system to collect income tax from revenues other than wages and pensions.

records.[54] By June 2019, HMRC had complied[55] and changed its way of seeking users' consent.[56]

The robustness of voice verification systems was questioned in 2023 when journalists reported they accessed the Australian Government's Centrelink[p] voice verification system using a voice generated with artificial intelligence (AI).[q 59]

To detect AI-generated voices, Nuance Communications,[r] a Microsoft company developing voice verification systems, combined voice verification with synthetic speech detection[s] and conversational algorithms.[t 63] Nuance Communications claims that the combination of these three technologies could accurately detect cloned voices in 99% of cases.[63]

# Biometric identification

Biometric identification, also known as 'one-to-many comparison', refers to the use of biometric data to determine whether an individual matches the information in a reference database.[3,39] By searching against a database of previously enrolled individuals, biometric identification asks "Who is this person?" or "Do we know this person already?".[39]

## Facial recognition

### Available facial recognition systems

Facial recognition may be used by UK police forces in situations in which it may be difficult for police officers to identify suspects, for instance in dense crowds.[64] There are three types of facial recognition (FR) systems used by UK police forces:

- **Retrospective Facial Recognition** (RFR) is a post-event[u] use of facial recognition technology that compares a facial image of an unknown individual against a reference image database (for instance, the Police National Database).[v]

---

[p] Centrelink is an Australian Government's agency providing social security payment and services.[57]

[q] Other AI attacks are increasing in frequency; one report stated that attacks in which a user's face is used in place of a malicious actor's own, via 'face swapping' AI software, increased by over seven times between 2022 and 2023.[58]

[r] Nuance Communications provides voice verification systems to the Australian Tax Office,[60] Natwest Group,[33] Lloyds Banking group,[32] and HSBC UK.[61] HMRC used Nuance's digital assistants to roll out HMRC's Covid-19 schemes to financially support businesses and individuals during the pandemic.[62]

[s] Synthetic speech detection algorithms detect tiny differences that distinguish a computer-generated voice from a live human voice.[63]

[t] Conversational algorithms analyse the way people use language (word choices, grammar, sentence structure) and compare it to the conversational patterns of known customers.[63]

[u] The EU AI Act uses the term "post" instead of "retrospective" for post-event use of biometric identification.[65]

[v] As of October 2023, there were 16,572,608 custody facial images held on the Police National Database.[17] In his Annual Report 2020, the Commissioner for the Retention and Use of Biometric

[67] For each identification search, the system returns a candidate list that best matches the submitted image.[67]

- **Operator Initiated Facial Recognition** (OIFR) is a near-real-time use of facial recognition technology, where a police officer takes a photograph of a subject via a mobile device and submits it for an immediate search against a reference image database.[67] For each identification search, the system returns a short candidate list that best matches the submitted image.[67] As of September 2024, OIFR is at an early trial stage.[64]

- **Live Facial Recognition**[w] (LFR) compares a live camera video feed of faces against a predetermined watchlist to find a possible match that generates an alert.[64]

### Facial recognition and the false positive rate

When a biometric system matches an individual with someone on a reference database who is not them, it is a 'false positive match'. The 'false-positive rate' of a system, also known as 'false alert rate', indicates how often a system generates a false positive match.

Facial recognition (FR) technology requires AI algorithms that have been trained on a dataset of known images. If the FR system has been trained on a dataset where certain types of face are under-represented, such as female faces or those from minority ethnic groups, the system will make errors more often when exposed to these under-represented faces.[68]

In 2023, the Metropolitan Police Service and the South Wales Police commissioned the National Physical Laboratory (NPL) to assess the LFR, RFR, and OIFR systems they used.[67] The objective of this study was to evaluate any bias and to determine the appropriate face-match thresholds[x] to ensure those systems perform with high accuracy and fairness.[67]

For low face-match thresholds, the NPL study found that there was a "statistically significant imbalance between demographics", with more Black or Asian subjects having a false positive than White subjects for live facial recognition.[y] [67]

In 2019, the US National Institute of Standards and Technology (NIST) conducted tests to quantify demographic differences for 52 face identification systems. The

---

Material wrote that most UK police officers were "continuing to retain the vast majority of their custody images indefinitely, regardless of whether the individual has been convicted of an offence".[66]

[w] The EU AI Act uses the term "real-time" instead of "live" when the biometric data capture, comparison, and identification all occur "without a significant delay".[65]

[x] A high face-match threshold makes the comparison algorithm stricter, increasing the risk that an offender won't be identified (false negative). A low threshold makes the comparison algorithm less strict, increasing the risk of matching an innocent person with an individual on an offender watchlist (false positive).[69]

[y] Out of 4,000 recognition opportunities against a demographically balanced dataset of 178,000 images using lower face-match thresholds than default settings, there were three White, eight Asian, and 22 Black subjects that had a false positive identification.

accuracy of these systems was evaluated against a database containing millions of faces from 24 countries in 7 distinct global regions.[70]

This study found that:

- False positives were higher in women than men. This effect is smaller than that due to race.[70]
- There were more false positives for the elderly and children in comparison to middle-age faces.[70]
- False positive rates were highest in West and East African, and East Asian people, and lowest in Eastern Europe individuals. However, this effect was reversed for East Asian people for several algorithms developed in China.[70]

## Fingerprints and forensics

Forensics, also known as forensic science, is the application of scientific methods to matters of criminal and civil law.[71] Forensics can be used, for example, to establish a person's presence at the scene of a crime, exclude a suspect from a scene, or link different crime scenes to provide intelligence on crime patterns.[72]

Forensic analysis can be supported by biometric information, such as fingerprints.[72] The first criminal trial in the United Kingdom in which a person was identified and convicted based on fingerprint evidence took place in 1902.[73]

In 2022, the National Police Chiefs' Council deployed the Police Digital Service (PDS) Xchange platform.[74] This national cloud-based platform integrates the existing UK national fingerprints database IDENT1[z] - comprising 8.6 million digital fingerprint records – and allows forensic teams to access this database remotely to send fingerprints in real-time for comparison and identification.[74]

# New generation biometric systems

New systems have been developed that aim to classify individuals into different demographic categories or infer emotions and psychological states (Box 2).[17] These systems use correlations between biometric characteristics, such as facial features, and traits, such as age or race, based on AI models analysing patterns from large datasets.[76]

## Biometric categorisation system

Biometric categorisation systems[aa] seek to categorise individuals based on biometric data collected and compared with features on large databases.[17] For example, biometric systems have been developed to categorise people according to their gender,[77] age,[77] ethnicity,[78] body mass index,[79] or sexuality.[80–82]

[z] Since 2012, IDENT1 is operated by the Home Office and is accessible by law enforcement agencies.[75]

[aa] Also known as biometric classification systems.

Some of these systems, in particular those related to sexuality, have been highly criticised by researchers[83,84] and think tanks[19,18,17] for using pseudo-scientific assumptions[bb] to draw links between facial features and other traits.[83,84]

## Biometric inferential systems

Biometric inferential systems infer a person's emotions or behaviour based on biometric data.[17] For example, with the increase in online learning during the pandemic, Intel developed a system that it claims can detect whether students in online classes are bored or paying attention based on student's facial expressions.[86,87] Academics and think tanks[17–19,88] have also expressed concerns over the use of biometric inferential system during job interviews (Box 2).

### Box 2: Controversial uses of facial recognition

- **Clearview AI** is a US-based facial recognition company which offers a "face search" capability against its database of more than 40 billion facial images.[89] In 2022, the French,[90] Italian,[91] and Greek[92] data regulators all fined Clearview AI €20 million, the maximum fine possible for data breach under the EU GDPR. The ICO also issued an enforcement notice ordering the company to delete the data of UK residents from its systems.[19,20,93]
- **Hikvision and Dahua** are two Chinese state-owned surveillance camera makers providing facial recognition software. In April 2022, in a letter to the Cabinet Office, the Biometrics and Surveillance Camera Commissioner (BSCC) highlighted the risk presented by "state-controlled surveillance systems covering our public spaces".[94,95] In November 2022, the UK Government instructed government departments to stop using Chinese CCTV systems on sensitive sites.[96–98]

**HireVue** is a US-based company developing recruitment software used by more than 1,150 businesses.[99] HireVue's hiring software analysed thousands of data points related to a person's voice and facial movements to infer the candidate's "willingness to learn" and "personal stability".[100] In 2019, the American Electronic Privacy Information Center filed a complaint with the Federal Trade Commission alleging that "HireVue has committed unfair and deceptive practices".[100,101] Recruitment software using facial and voice recognition were found to penalise candidates with darker skin[102] or accents.[103] In 2021, HireVue announced that it would stop relying on facial analysis to assess job candidates.[104]

[bb] Such as physiognomy, a pseudoscience investigating the systematic correspondence of psychological characteristics to physical features.[85]

# UK regulatory environment for biometric data

After the UK left the European Union (EU), the key principles, rights and obligations of the EU GDPR were retained in domestic law as UK GDPR.[cc] [16] However, leaving the EU had implications on the rules on transfers of personal data from the European Economic Area (EEA) to the UK, described below.[dd] [16]

## Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) updated data protection laws in the UK.[ee] It supplements the EU GDPR, implements the Law Enforcement Directive (LED), and extended data protection laws to areas that are not covered by the EU GDPR or the LED such as intelligence services.[105,106]

On 28 June 2021, the EU Commission published two adequacy decisions[ff] in respect of transfers of personal data from the EEA to the UK:[108,109]

- **EU GDPR adequacy decision**: This decision states that the UK provides adequate protection for personal data transferred from the EEA to the UK under the EU GDPR.[110,111]

- **Law Enforcement Directive adequacy decision**: This decision states that the UK provides adequate protection for personal data transferred from EU law enforcement authorities.[111,112]

These two adequacy decisions allow personal data, such as biometric data, to move freely from the EEA to the UK.[108,109] The adequacy decisions also support the implementation of the EU-UK Trade and Cooperation Agreement.[gg] [108,109]

Both adequacy decisions include safeguards in case of future divergence between the UK and the EU such as a "sunset clause", which limits the duration of adequacy to four years.[108] These two adequacy decisions are expected to last until 27 June 2025 at which point they could be extended for another four years.[111]

[cc] The UK has the independence to amend and keep under review the UK GDPR.[16]

[dd] The EEA includes the 27 EU countries alongside Iceland, Liechtenstein, and Norway.

[ee] Past UK regulations include: the Data Protection Act 1984, Data Protection Act 1998, and the Privacy and Electronic Communications Regulations 2003.

[ff] An adequacy decision is a decision made by the EU which recognises that another country provides an equivalent level of protection for personal data to the EU.[107]

[gg] The EU-UK Trade and Cooperation Agreement sets out arrangements in areas such as trade, digital trade, intellectual property, public procurement, transport, energy, law enforcement and judicial cooperation in criminal matters.[113,114]

# UK regulators

## Information Commissioner's Office

The Information Commissioner's Office (ICO)[hh] was established to oversee the UK-wide application of the Data Protection Act 1984.[119] The ICO is an executive non-departmental public body sponsored by the Department for Science, Innovation and Technology.[120] The ICO is primarily funded by organisations paying the data protection fee,[ii] which covers over 85% of the ICO's annual budget of £87.3 million in 2023-24.[121]

The ICO ensures individuals' rights are protected under data protection regulations (for instance, DPA 2018, UK GDPR).[122] It can take legal actions against non-compliant organisations, including biometric data collection, use and storage (Box 2).[123] As data protection legislation is not devolved to Wales, Scotland, or Northern Ireland, the ICO's remit covers the UK as a whole.[124,125]

## Home Office bodies

### Office of the Biometrics and Surveillance Camera Commissioner

The Protection of Freedoms Act 2012 established two statutory roles:

- **The Commissioner for the Retention and Use of Biometric Material** reviews the retention and use of DNA samples, DNA profiles and fingerprints by the police.[126]
- **The Surveillance Camera Commissioner** encourages compliance with the Home Secretary's voluntary Surveillance Camera Code of Practice.[jj] [128]

Since 2022, the two posts have been carried out by one full-time Biometrics and Surveillance Camera Commissioner (BSCC).[128]

The BSCC is an independent monitoring body of the Home Office.[129] The commissioner has no enforcement or inspection powers and works with relevant authorities to ensure they follow the Surveillance Camera Code of Practice.[129]

In 2023 the UK Government put forward the Data Protection and Digital Information (DPDI) Bill, which proposed to abolish the BSCC's office. The removal of the BSCC's office has been criticised by academics[124] and think tanks.[130,131] The bill did not complete all its stages before the 2024 general election.

---

[hh] Also known as the Data Protection Registrar until 2001, the Information Commissioner's Office also publishes investigations and opinions on UK data, for instance on facial recognition technology.[115–118]

[ii] Under the DPA 2018, organisations processing personal data must pay a data protection fee.[121]

[jj] The purpose of this code is "to enable operators of surveillance camera systems to make a legitimate use of this technology in a way that the public would rightly expect and to a standard that maintains public trust and confidence."[127]

### Biometrics and Forensics Ethics Group

The Biometrics and Forensic Ethics Group (BFEG) was formed in 2017 as a successor to the National DNA Database Ethics Group.[132] The BFEG is an advisory non-departmental public body sponsored by the Home Office.[132] The BFEG is structured as a committee comprising experienced unpaid professionals with expertise in, for instance, computer or forensic science, or law.[kk] [134]

The BFEG is commissioned to consider the ethical impact on society, groups, and individuals in areas such as: the collection, retention, and use of human biometric identifiers (DNA, fingerprints, face recognition), the retention and use of forensic data, the use of large datasets within the Home Office, and the implementation of systems using AI.[135]

The BFEG has published various briefing notes on, for instance, the ethical issues arising from voice analysis or public-private collaboration in the use of live facial recognition technology.[136]

A BFEG interim report from 2019 found that there was a need to differentiate biases "inherent to the design and training" of LFR models from biases "introduced when a human operator decides on the basis of the system output."[68] This report also highlighted "the lack of independent oversight and governance of the use of LFR", recommending "that police trials of LFR should comply with the usual standards of experimental trials" until the development of a LFR legislative framework.[68]

## Scottish Biometric Commissioner

Investigation of crime, maintenance of public order, and policing in Scotland is devolved to the Scottish Parliament.[ll] [125,137,138] The Scottish Biometrics Commissioner Act 2020 established the Office of the Scottish Biometric Commissioner, which has oversight over the collation, use, and storage of biometric data by Police Scotland.[mm] [6,139]

The Commissioner's function is to promote the adoption of lawful, effective, and ethical practices regarding the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes.[139] The Commissioner's function extends to Police Scotland, the Scottish Police Authority and the Police Investigations and Review Commissioner.[139]

The Commissioner has prepared a Code of Practice on the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes, which entered into force in November 2022.[140] The office of the Scottish Biometric Commissioner publishes annual reports, guidance, and reviews. In 2023, a review on the acquisition of biometric data from children and vulnerable persons in custody

[kk] The BFEG also has a representative on the Forensic Information Databases Strategy Board, which provides oversight over the National DNA Database (NDNAD) and the National Fingerprint Database (IDENT1).[133]

[ll] Surveillance by Police Scotland and devolved public authorities is devolved, but other surveillance carried out by security and intelligence agencies (among others) is reserved.[125]

[mm] The Scottish Biometrics Commissioner is independent of the Scottish Government and is appointed by His Majesty the King on the nomination of the Scottish Parliament.[139]

found that the information the police gives to individuals when taking biometric data should be tailored to the needs of the recipient.[141]

The Scottish Biometric Commissioner's remit only covers the use and retention of biometric data in Scotland for policing and criminal purposes.[nn] The use and retention of biometric data in Scotland for national security purposes is not devolved to Scotland and is part of the BSCC's remit.[124]

# Digital Information and Smart Data Bill

In 2024, the King's Speech outlined plans for a Digital Information and Smart Data Bill that may have implications for the use of biometric data in the UK. The government said the bill would establish a Digital Verification Service to create secure digital identity products for pre-employment checks or moving house, for instance, and to "ensure [public] data is well protected by giving the regulator (the ICO) new, stronger powers and a more modern structure."

Information on the bill will be published on the parliament website when it is introduced.

# International regulatory environment for biometric data

## EU General Data Protection Regulation

The EU General Data Protection Regulation (EU GDPR) is an EU law that protects fundamental rights affected by the processing of personal data. This law came into effect in the EU in 2018.[oo] The EU GDPR imposes obligations on organisations within and outside of the EU that use or collect personal data of individuals in the EU.[105]

The EU GDPR allows supervisory authorities to issue substantial fines for non-compliant organisations, including for biometric data misuse (Box 2). These fines can be as high as €20 million (£17 million)[pp] or 4% of the company's annual global revenue, whichever is higher.[2] Notable financial penalties for non-compliance included £1 billion levied against Meta Platforms Ireland by the Data Protection Authority of Ireland, which found that it had unlawfully transferred personal customer data to Meta US.[144,145]

[nn] Extending only to the use of fingerprints and DNA of non-convicted persons.

[oo] The EU GDPR applied in the UK from 25 May 2018 until the end of the implementation period of the UK-EU Withdrawal Agreement on 31 December 2020.[142]

[pp] As of September 2024, the Bank of England's exchange rate against Euro is: £0.84.[143]

# The Law Enforcement Directive

The Law Enforcement Directive (LED) is an EU directive that sits alongside the EU GDPR. The LED deals with the processing of personal data by data controllers for "law enforcement purposes", which falls outside of the scope of the EU GDPR. In particular, the LED ensures that personal data of victims, witnesses, and suspects of crime are protected. The LED also facilitates cross-border cooperation in addressing crime and terrorism.[105]

# AI and biometric data: international comparison

Developments in AI have led to the emergence of new possible uses of biometric data. AI-assisted tools can recognise faces with a similar efficiency to the human brain[146] and the identity of an individual can be quickly verified with a short voice recording.[34,32,33,30,60] The potential consequences have led many leading jurisdictions and their regulators to focus increasing attention on AI.

- **UK pro-innovation approach to AI regulation**: In March 2023, the UK Government published a white paper introducing its regulatory framework for the use of AI.[147] This 'context-based' framework relies on existing regulators to assess the impact of AI on individuals in a particular context.[148] In February 2024, the UK Government published the outcome of its consultations on AI and confirmed its intention to pursue its pro-innovation approach.[149] The Data Protection and Digital Information (DPDI) Bill was introduced by the Government in March 2023 to update provisions on the oversight of biometric data, but it fell at the 2024 general election.[150,151]

- **US Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence**: In October 2023, the US President issued an Executive Order regulating the use of AI in the US.[152] This Executive Order establishes an AI 'risk-based' approach and directs various federal agencies and departments to create standards and regulations for the use or oversight of AI.[153,154]

- **EU AI Act**: This Act came into force on 1 August 2024[qq] and gives provision for a 'risk-based' approach. It lays out comprehensive rules across all sectors and applications.[148,156,157] It establishes four levels of risk of AI to fundamental human rights (unacceptable risk, high risk, limited risk, and minimal risk), with different rules for each level.[148] The use of biometric identification systems is prohibited for law enforcement except in "narrowly defined situations."[158]

A detailed comparison on the regulation of biometric data and AI across the UK, EU and US is provided in Table 2 below.

[qq] Regulation (EU) 2024/1689.[155]

| Table 2: Comparison of EU, US, and UK regulation of use of AI and biometric data | | | |
|---|---|---|---|
| | **EU AI Act[159,160]** | **US Executive Order on AI[152]** | **UK Regulations** |
| **Facial recognition (FR)** | Forbids the compiling of FR databases by "untargeted scraping of facial images from the internet or CCTV footage".[161]<br><br>Forbids the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement.[rr] [161] | No mention of FR in the Executive Order.<br><br>The accuracy and fairness of facial recognition software continues to be evaluated by the NIST's Face Recognition Vendor Test.[162] | The DPA 2018 gives provision for the oversight of the use of FR for both the private sector and police under certain conditions.[163] |
| **Biometric categorisation and inferential systems** | Forbids the use of systems that categorise individuals "based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation".[161] | Federal governments must ensure a lawful, safe, and secure handling of data when used for inferring information about people's habits and desires.[152]<br><br>Federal governments must also mitigate privacy and confidentiality risks.[152] | From 2023, the ICO is working on a consultation on "biometric classification and data protection".[164,165] |
| **New regulators** | AI Office: monitors, supervises, and enforces the EU AI Act, analyses unforeseen risks, and supports the creation of regulatory sandboxes[ss] where companies can test AI systems in a controlled environment.[168] | AI Safety and Security Board: advises the Secretary of Homeland Security, private sector stakeholders, and the public on the safe and secure development and deployment of AI technology.[169] | The DPDI Bill, which fell at the 2024 election, provided for the transfer of the offices of Commissioner for the Retention and Use of Biometric Material and Surveillance Camera to the Investigatory Powers Commissioner's Office (IPCO).[tt] [124] |

[rr] Except when: searching for missing persons, searching for trafficked or sexually exploited persons, for preventing threat to life, for preventing terrorist attack, for identifying suspects in serious crimes.

[ss] A regulatory sandbox is a controlled environment where AI systems can be developed, tested, and validated before being released to the market. A regulatory sandbox provides innovators with incentives to test their innovations in a controlled environment and allows regulators to better understand the technology.[166,167]

[tt] The Investigatory Powers Act 2016 established the IPCO which provides oversight of the use of investigatory powers by intelligence agencies, police forces and other public authorities.

# References


1. Department for Digital, Culture, Media & Sport (2018). Data Protection Act 2018, c.12.
2. European Parliament (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
3. International Organization for Standardization (2022). ISO/IEC 2382-37, Information technology - Vocabulary - Part 37: Biometrics.
4. Biometric Institute (2024). Types of Biometrics - DNA.
5. Home Office (2012). Protection of Freedoms Act 2012. *c.9*.
6. Scottish Government (2020). Scottish Biometrics Commissioner Act 2020.
7. Scottish Biometrics Commissioner (2024). What Are Biometrics?
8. Information Commissioner's Office (2022). Biometrics: insight.
9. Information Commissioner's Office (2022). Biometrics: foresight.
10. Shanbhag, A. (2024). What Is an Authenticator App and How Does One Work? *Lifewire*.
11. FIDO Alliance (2023). 2023 Online Authentication Barometer.
12. Security (2022). Over half of consumers use biometrics to secure mobile devices.
13. Grand View Research (2022). Passwordless Authentication Market Size & Share Report, 2030.
14. Expert Market Research (2024). Global Passwordless Authentication Market Report and Forecast 2024-2032.
15. Information Commissioner's Office (2023). Special category data.
16. Information Commissioner's Office (2019). The UK GDPR.
17. Stockwell, S. *et al.* (2024). The Future of Biometric Technology for Policing and Law Enforcement: Informing UK Regulation. Centre for Emerging Technology and Security.
18. Ryder KC, M. (2022). The Ryder Review: Independent legal review of the governance of biometric data in England and Wales. Ada Lovelace Institute.
19. Chang, M. (2022). Countermeasures: the need for new legislation to govern biometric technologies in the UK. Ada Lovelace Institute.
20. Big Brother Watch (2023). Biometric Britain: The Expansion of Facial Recognition Surveillance.
21. Stevens, A. *et al.* (2023). 'I started seeing shadows everywhere': The diverse chilling effects of surveillance in Zimbabwe. *Big Data & Society*, Vol 10, 20539517231158631. SAGE Publications Ltd.
22. Loideain, N. N. (2024). Lawfulness and Police Use of Facial Recognition in the United Kingdom: Article 8 ECHR and Bridges v. South Wales Police. in *The Cambridge Handbook of Facial Recognition in the Modern State*. (eds. Zalnieriute, M. et al.) 155–172. Cambridge University Press.
23. Holder, E. H. *et al.* (2011). The Fingerprint Sourcebook. National Institute of Justice.
24. Apple Inc. (2023). About Touch ID advanced security technology.
25. Triggs, R. (2024). How fingerprint scanners work: Optical, capacitive, and ultrasonic explained. *Android Authority*.
26. Microsoft Support (2024). Configure Windows Hello.
27. Shultz, D. (2015). When your voice betrays you. *Science*, Vol 347, 494–494.
28. Nuance (2015). The essential guide to voice biometrics.

29. Moss, J. (2024). Biometrics Are Proving Increasingly Essential for Banking Security. *International Banker*.
30. HSBC UK Bank plc. (2020). HSBC UK Launches New Voice-Driven Technology.
31. Thompson, B. (2016). HSBC offers voice and fingerprint ID system to customers. *BBC News*.
32. Mayhew, S. (2018). Lloyds Banking Group deploys Nuance voice biometrics. *BiometricUpdate.com*.
33. Nuance (2021). NatWest Group fights fraud and improves customer experiences.
34. HM Revenue & Customs (2017). Voice ID showcases latest digital development for HMRC customers.
35. Apple Inc. (2024). About Face ID advanced technology.
36. Border Force (2024). Guide to faster travel through the UK border.
37. Biometrics Institute (2024). Biometric verification and identification explained.
38. Kubota, Y. (2017). Apple iPhone X Production Woe Sparked by Juliet and Her Romeo. *Wall Street Journal*.
39. Information Commissioner's Office (2024). Biometric recognition.
40. Information Commissioner's Office (2024). How do we keep biometric data secure?
41. National Cyber Security Centre (2019). Biometric recognition and authentication systems.
42. National Cyber Security Centre (2021). Device Security Guidance.
43. Information Commissioner's Office (2023). Right to erasure.
44. Information Commissioner's Office (2024). How do we consider rights requests for biometric data?
45. HM Passport Office (2022). Basic passport checks.
46. Office for National Statistics (2022). International migration, England and Wales: Census 2021.
47. Thales (2022). New ABC eGates: Compact, Modular, and Efficient.
48. Dann, S. (2023). Border Force letter about eGates.
49. Peachey, K. (2016). Banks turning to voice recognition. *BBC News*.
50. HSBC UK Bank plc. (2020). HSBC UK's VoiceID prevents £400m of attempted fraud.
51. Simmons, D. (2017). BBC fools HSBC voice recognition security system. *BBC News*.
52. HM Revenue & Customs (2019). Freedom of Information Act 2000 (FOIA).
53. Big Brother Watch (2019). Tax Voice ID scheme faces backlash as thousands delete Voice IDs.
54. Information Commissioner's Office (2019). Her Majesty's Revenue and Customs (HMRC) – ICO Data Protection Audit Executive Summary.
55. Peachey, K. (2019). HMRC forced to delete five million voice files. *BBC News*.
56. HM Revenue & Customs (2018). Voice Identification Privacy Notice.
57. Australian Government (2023). Centrelink.
58. iProove (2024). Threat Intelligence Report 2024.
59. Evershed, N. *et al.* (2023). AI can fool voice recognition used to verify identity by Centrelink and Australian tax office. *The Guardian*.
60. Nuance (2018). Australian Tax Office deploys voice biometrics.
61. Pascu, L. (2020). HSBC UK's voice biometrics system blocked 2x more fraud attempts in 2019. *Biometric Research Group, Inc.*
62. Nuance (2021). HMRC adapts to COVID-19 with support from Nuance.
63. Beranek, B. (2023). How Gatekeeper biometric authentication detects and beats synthetic voices. *Nuance What's Next blog*.
64. Home Office (2023). Police use of Facial Recognition: Factsheet.

65. European Parliament, Council of the European Union (2024). Article 3: Definitions.
66. Sampson, F. (2021). Biometrics Commissioner Annual Report 2020. Office of the Biometrics and Surveillance Camera Commissioner.
67. Mansfield, T. (2023). Facial Recognition Technology in Law Enforcement, Equitability Study, Final Report. National Physical Laboratory.
68. Biometrics and Forensics Ethics Group (2019). Police use of live facial recognition technology: ethical issues. *GOV.UK*.
69. Fiumara, G. (2022). A Tale of Two Errors: Measuring Biometric Algorithms. *National Institute of Standards and Technology*.
70. Grother, P. *et al.* (2019). Face recognition vendor test part 3: demographic effects. NIST IR 8280. National Institute of Standards and Technology.
71. Siegel, J. A. (2024). Forensic science. *Encyclopaedia Britannica*.
72. College of Policing (2017). Forensics.
73. Galloway, V. *et al.* (2007). Fingerprints. in *Forensic human identification : an introduction*. CRC Press.
74. Police Digital Service (2022). A new digital fingerprint capability for policing.
75. Home Office (2023). Forensic Information Databases annual report 2021 to 2022.
76. Yurdasen, D. (2023). How Artificial Intelligence (AI) Is Used In Biometrics. *Aratek*.
77. Abirami, B. *et al.* (2020). Gender and age prediction from real time facial images using CNN. *Materials Today: Proceedings*, Vol 33, 4708–4712.
78. Masood, S. *et al.* (2018). Prediction of Human Ethnicity from Facial Images Using Neural Networks. in *Data Engineering and Intelligent Computing*. (eds. Satapathy, S. C. et al.) 217–226.
79. Wen, L. *et al.* (2013). A computational approach to body mass index prediction from face images. *Image and Vision Computing*, Vol 31, 392–400.
80. Wang, Y. *et al.* (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of Personality and Social Psychology*, 246–257.
81. The Economist (2017). Advances in AI are used to spot signs of sexuality.
82. Levin, S. (2017). New AI can guess whether you're gay or straight from a photograph. *The Guardian*.
83. Bowyer, K. W. *et al.* (2020). The "Criminality From Face" Illusion. *IEEE Transactions on Technology and Society*, Vol 1, 175–183.
84. Vincent, J. (2017). The invention of AI 'gaydar' could be the start of something much worse. *The Verge*.
85. Encyclopaedia Britannica (2023). Physiognomy.
86. Knight, W. (2021). Job Screening Service Halts Facial Analysis of Applicants. *Wired*.
87. Pires, F. (2022). Intel Develops Controversial AI to Detect Emotional States of Students. *Tom's Hardware*.
88. Bogen, M. *et al.* (2018). Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias. Upturn.
89. Clearview AI, Inc. (2024). Company Overview.
90. Lomas, N. (2022). France fines Clearview AI maximum possible for GDPR breaches. *TechCrunch*.
91. Lomas, N. (2022). Italy fines Clearview AI €20M and orders data deleted. *TechCrunch*.
92. Lomas, N. (2022). Clearview AI hit with another €20M ban order in Europe. *TechCrunch*.
93. Information Commissioner's Office (2022). ICO fines facial recognition

database company Clearview AI Inc more than £7.5m and orders UK data to be deleted.
94. Fraser Sampson (2022). Letter to Rt. Hon. Michael Gove MP: Human Rights and Security Issues in Public Procurement of Surveillance Technology.
95. Office of the Biometrics and Surveillance Camera Commissioner (2024). Biometrics and Surveillance Camera Commissioner Annual Report – 2022/2023.
96. Dowden, O. (2022). Security Update on Surveillance Equipment. UK Parliament.
97. Baroness Neville-Rolfe (2022). Security Update on Surveillance Equipment. UK Parliament.
98. Yang, Y. *et al.* (2023). UK to strip Chinese surveillance cameras from sensitive government sites. *Financial Times*.
99. HireVue (2024). New HireVue survey unveils shift: Forward-thinking hiring leaders prioritize potential over past experience.
100. Harwell, D. (2019). Rights group files federal complaint against AI-hiring firm HireVue, citing 'unfair and deceptive' practices. *Washington Post*.
101. Electronic Privacy Information Center (2019). In re HireVue.
102. Buolamwini, J. *et al.* (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. in *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*. 77–91. PMLR.
103. Harwell, D. (2018). The accent gap: How Amazon's and Google's smart speakers leave certain voices behind. *The Washington Post*.
104. Electronic Privacy Information Center (2021). HireVue, Facing FTC Complaint From EPIC, Halts Use of Facial Recognition. *epic.org*.
105. European Commission (2023). Data protection in the EU.
106. Information Commissioner's Office (2019). An overview of the Data Protection Act 2018.
107. European Commission (2016). Adequacy decisions.
108. European Commission (2021). Data protection: Commission adopts adequacy decisions for the UK.
109. Department for Digital, Culture, Media and Sport (2021). EU adopts 'adequacy' decisions allowing data to continue flowing freely to the UK.
110. European Commission, Directorate-General for Justice and Consumers (2021). Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. *Official Journal L*. Vol 360, 1–68.
111. Information Commissioner's Office (2019). Adequacy.
112. European Commission, Directorate-General for Justice and Consumers (2021). Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. *Official Journal L*. Vol 360, 69–107.
113. European Commission (2021). The EU-UK Trade and Cooperation Agreement. *European Commission*.
114. Foreign, Commonwealth and Development Office (2021). UK/EU and EAEC: Trade and Cooperation Agreement.
115. Information Commissioner's Office (2020). Our history.
116. Information Commissioner's Office (2019). The use of live facial recognition technology by law enforcement in public places.
117. Information Commissioner's Office (2021). The use of live facial recognition technology in public places.

118. Information Commissioner's Office (2019). ICO investigation into how the police use facial recognition technology in public places.
119. Information Commissioner's Office (2021). History of the ICO.
120. UK Government (2021). Information Commissioner's Office.
121. Information Commissioner's Office (2024). How we are funded.
122. Information Commissioner's Office (2023). Information Commissioner's Annual Report and Financial Statements 2022/23.
123. Information Commissioner's Office (2022). Enforcement action.
124. Fussey, P. *et al.* (2023). Changes to the functions of the BSCC: independent report. Biometrics and Surveillance Camera Commissioner.
125. Torrance, D. (2022). Reserved matters in the United Kingdom. House of Commons Library.
126. Office of the Biometrics Commissioner (2024). About us.
127. Home Office (2021). Surveillance Camera Code of Practice.
128. UK Government (2021). Surveillance Camera Commissioner.
129. Biometrics and Surveillance Camera Commissioner (2024). About us.
130. Matt, D. (2024). It's time to strengthen data protection law for the AI era. *Ada Lovelace Institute*.
131. Big Brother Watch (2023). Big Brother Watch Briefing on the Data Protection and Digital Information 2.0 Bill for House of Commons Second Reading.
132. Biometrics & Forensic Ethics Group (2023). Biometrics and Forensics Ethics Group. Guidance: Information sheet.
133. UK Government (2024). Forensic Information Databases Strategy Board.
134. Biometrics and Forensic Ethics Group (2024). Membership.
135. Biometrics and Forensic Ethics Group (2024). About us.
136. Biometrics and Forensic Ethics Group (2021). Briefing note on the ethical issues arising from public–private collaboration in the use of live facial recognition technology.
137. The Scottish Parliament (2024). Devolved and Reserved Powers.
138. Paun, A. *et al.* (2020). Criminal justice and devolution. *Institute for Government*.
139. Scottish Biometrics Commissioner (2024). What we do.
140. Scottish Biometrics Commissioner (2022). Code of Practice.
141. Scottish Biometrics Commissioner (2023). Joint Assurance Review on the acquisition of biometric data from vulnerable persons.
142. UK Government (2020). EU legislation and UK law.
143. Bank of England (2024). Daily spot exchange rates against Euro.
144. Data Protection Commission (2023). Data Protection Commission announces conclusion of inquiry into Meta Ireland.
145. European Data Protection Board (2023). 1.2 billion euro fine for Facebook as a result of EDPB binding decision.
146. Michalowski, J. (2022). An optimized solution for face recognition. *MIT News*.
147. Department for Science, Innovation and Technology (2023). A pro-innovation approach to AI regulation.
148. Roberts, H. (2023). AI in the EU and UK: two approaches to regulation and international leadership. *UK in a Changing Europe*.
149. Department for Science, Innovation and Technology (2024). A pro-innovation approach to AI regulation: government response.
150. UK Parliament (2024). Data Protection and Digital Information Bill.
151. British Retail Consortium (2024). General Election 2024: Bills saved and lost during 'wash up'.
152. Executive Office of the President (2023). Executive Order on the

Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.
153. Engler, A. (2023). The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment. *Brookings*.
154. Morrison, S. (2023). President Biden's new plan to regulate AI. *Vox*.
155. European Parliament, Council of the European Union (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations.
156. Borak, M. (2024). EU publishes rollout schedule for AI Act. *BiometricUpdate.com*.
157. Sato, M. (2024). The AI Act compliance countdown begins. *The Verge*.
158. European Parliament (2024). Artificial Intelligence Act: committees confirm landmark agreement.
159. Council of the European Union (2024). Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI.
160. European Parliament (2024). European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.
161. European Parliament (2024). Article 5: Prohibited Artificial Intelligence Practices.
162. National Institute of Standards and Technology (2020). Face Recognition Vendor Test (FRVT).
163. Centre for Data Ethics and Innovation (2020). Snapshot Paper - Facial Recognition Technology.
164. Information Commissioner's Office (2023). ICO consultation on the draft biometric data guidance.
165. Information Commissioner's Office (2024). Biometric data guidance: Biometric recognition.
166. European Parliament (2024). Article 57: AI Regulatory Sandboxes.
167. European Parliament (2022). Artificial intelligence act and regulatory sandboxes.
168. EU Artificial Intelligence Act (2024). The AI Office: What is it, and how does it work?
169. The White House (2024). Biden-Harris Administration Announces Key AI Actions 180 Days Following President Biden's Landmark Executive Order.

# Contributors

POST is grateful to Vincent Saverat for researching this briefing, to the Engineering and Physical Sciences Research Council for funding his parliamentary fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Simon Brawley.

POSTnotes are based on literature reviews and interviews with a range of stakeholders and are externally peer-reviewed. POST would like to thank interviewees and peer reviewers for kindly giving up their time during the preparation of this briefing, including:

Members of the POST Board*

Matt Davies, Ada Lovelace Institute

Ian Deasha, Information Commissioner's Office*

Professor Mark Elliot, University of Manchester

Professor Pete Fussey, University of Essex

Sam Jefferies, United Nations High Commissioner for Refugees

Thomas Jensen, Milestone systems A/S

Dr Nóra Ní Loideáin, Information Law & Policy Centre

Brian Plastow, Scottish Biometrics Commissioner*

Diego Quiroz, Scottish Biometrics Commissioner Office

Dr Birgit Schippers, University of Strathclyde

Bruce Schneier, Harvard Kennedy School

Samuel Stockwell, Alan Turing Institute

Madeleine Stone, Big Brother Watch

Kai Zenner, European Parliament

*denotes people and organisations who acted as external reviewers of the briefing.

The Parliamentary Office of Science and Technology (POST) is an office of both Houses of Parliament. It produces impartial briefings designed to make research evidence accessible to the UK Parliament. Stakeholders contribute to and review POSTnotes. POST is grateful to these contributors.



If you have any comments on our briefings please email post@parliament.uk. Please note that we are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk or the House of Lords email hlinfo@parliament.uk.

DOI: https://doi.org/10.58248/PN731

Image Credit: Pixel-shot via Adobe Stock #502498760



post@parliament.uk
parliament.uk/post
@POST_UK